UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/084,859	02/27/2002	Melissa W. Dunn	MS# 180490.1 (MSFT 4969)	8746

321 7590 09/22/2005

SENNIGER POWERS LEAVITT AND ROEDEL
ONE METROPOLITAN SQUARE
16TH FLOOR
ST LOUIS, MO 63102

EXAMINER	
JOO, JOSHUA	

ART UNIT	PAPER NUMBER
2154	

DATE MAILED: 09/22/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/084,859	DUNN, MELISSA W.	
	Examiner	Art Unit	
	Joshua Joo	2154	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 July 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-46* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-46* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *7/14/2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

HC

Response to Office Action Filed on 7/7/2005

1. Claims 1-46 are presented for examination.

Information Disclosure Statement

2. The information disclosure statement (IDS) submitted 7/14/2005 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Claim Rejections - 35 USC § 112

3. Claim 24 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

i) As per claim 24, the claim is dependent on itself. For this office action, claim 24 will be considered as depending on independent claim 22.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 22, 24, 26, 28, and 40-41 are rejected under 35 U.S.C. 102(e) as being unpatentable by Desai #6,820,204 (Desai hereinafter).

6. As per claim 22, Desai teaches the invention as claimed including a computer-readable media for selectively granting clients access to a user's stored profile information. Desai's teachings comprise of:

identifying the user (Col 9, lines 19-28; Col 14, lines 63-65. Client requests access to user's stored profile information, e.g. vendor and telemarketer.);

identifying a plurality of clients of the web-services provider (Col 9, lines 13. One or more third parties) wherein the user desires to grant access to the user-specific information in the data store to certain of the plurality of clients (Col 8, lines 31-33; Col 9, lines 1-5; Col 14, lines 63-65. Client requests access to view user's stored profile information in an Internet network. Col 9, lines 12-13. User selectively grants access to one or more third parties.);

identifying a method of access by which the user is willing to allow the certain clients to access the user-specific information in the data store (Col 9, lines 9-14. User selectively grants access to one or more third parties. User allows clients to view information on an element-by-element bases.);

identifying a level of access to the user-specific information in the data store the user desires to impose on the certain clients (Col 9, lines 10-18. The user selectively grants access to the store profile information.); and

writing an access control rule to an access control list associated with said data store, said access control rule limiting access to the user-specific information in the data store by the certain clients to the identified method of access and the identified level of access (Col 9, lines 19-22; Col 13, lines 25-33. User writes an access control rule that limits access to the user

profile information by the identified method and level. Col 9, lines 9-14. User selectively grants access to one or more third parties.).

7. As per claim 40, Desai teaches the invention as claimed including a method for selectively granting clients access to user's stored profile information. Desai's teachings comprise of:

obtaining at the web-services provider a digital request message from the third party (Col 9, line 13. One or more parties) desiring access to the certain user-specific information in the data store (Col 8, lines 31-34; Col 9, lines 1-4; Col 14, lines 61-64. Client requests access to user's stored profile information, e.g. telephone number, street address, credit card number, where the user's stored profile information is stored on a web server.);

determining an intended purpose of third party accessing the certain user-specific information in the data store (Col 9, lines 19-31. Telemarketer, e.g. telemarketing.);

generating an option list having at least one entry therein based on the determined intended purpose of the third party for accessing the certain user-specific information in the data store (Col 9, lines 19-28; Col 13, lines 9-38. User generates a list based on purpose for the client to access user information. User allows vendor to view personal information while telemarketer is denied.);

displaying to the user on the display interface of the network communication device an option menu reflecting the generated option list, said option menu prompting the user to accept or reject at least one option using the selection interface of the network communication device (Col 8, lines 34-38, 63-65; Col 9, lines 27-31. User uses a computer running a web browser. User may selective grant access to each view to the clients. Telemarketer will be denied access to view user information.);

receiving from the network communication interface device a selection signal indicative of whether the user accepted or rejected the at least one option (Col 8, lines 63-65; Col 8, lines 27-31. User may selective grant access to each view to the clients. Telemarketer will be denied access to view user information.); and

creating an access control rule based on the received selection signal, said access control rule defining an extent of access to the certain user-specific information in the data store granted to the third party (Col 13, lines 8-32. User selectively grants access to allow one or more third parties access to element-by-element basis.).

8. As per claim 24, Desai teaches the method of claim 22 further comprising: exposing a menu to the user on the display interface of the network communication device, said menu allowing the user to identify the certain clients, the method of access, and the level of access; and transmitting the identified certain clients, the method of access, and the level of access to the web-services provider in a digital message format (Col 8, lines 34-38; Col 9, lines 10-30; Col 14, lines 7-15. Registered user uses a computer on a communication network. User may selectively grant access on an element-by-element basis for each view to one or more third parties. A vendor is granted view access to telephone number and address by providing an access code or password, while a telemarketer may not be granted view access.).

9. As per claim 26, Desai teaches the method of claim 22 wherein identifying the level of access further comprises grouping the user-specific information in the data store into a plurality of information types and identifying which of said plurality of information types the certain clients may access (Col 9, lines 10-30. The user-specific information in the data store is grouped and

identified as to which information the client may access. Vendor may access telephone number and credit card number, while business contact may just view the user's telephone number.).

10. As per claims 28 and 41, Desai teaches one or more computer-readable media having computer-executable instructions for performing the method recited in claim 22 (Col 11, lines 27-46. Information exchange system has software to perform necessary functions.).

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. Claim 23 is rejected under 35 U.S.C. 103(a) as being unpatentable over Desai in view of Robertson, US Patent #6,269,369.

13. As per claim 23, Desai teaches of selectively granting access to one or more third parties to user's stored profile. However, Desai does not teach the method of claim 22 further comprising identifying a subscription status, said subscription status indicating whether the user intends the certain clients to be notified if the user-specific information in the data store changes.

14. Robertson teaches of a contact management system, where clients may be permitted access to user's stored profile information. The contact manager determines whether any of the

user's contacts need to be notified of changes to the user's information (Col 6, lines 48-54; Col 8, lines 17-23, 57-61).

15. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Desai and Robertson because both teachings deal with providing selective access to user's profile information. Furthermore, the teachings of Robertson to selectively issue notification to the users in an access list would improve the teachings of Desai by allowing the user's clients to have the most up-to-date information regarding the user. The selective notification would allow the user to select clients that would receive notifications, allowing the user to maintain its privacy regarding its information.

16. Claims 25 and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Desai in view of Kramer et al, US Patent #5,414,852 (Kramer hereinafter).

17. As per claim 25, Desai does not teach the method of claim 22 wherein identifying the method of access further comprises identifying whether the certain clients is permitted to modify the user-specific information in the data store.

18. Kramer teaches of protecting data in a computer system, where the user permits the client to modify files in a data store (Col 4, lines 1-5, 52-55).

19. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Desai and Kramer because both teachings deal with providing security to files and selectively allowing access to the files. Furthermore, the teachings of Kramer for the user to permit the client to modify files in the data store would

improve the capability of Desai's teachings by allowing the user greater control of a client's type of access and allowing the client to update user's information.

20. As per claim 27, Desai does not teach the method of claim 22 further comprising: authenticating a digital identity of the user prior to writing the access control rule to the access control list associated with the data store of user-specific information; and writing the access control rule to said access control list if the digital identity of the user is authenticated.

21. Kramer teaches of providing an identifier to access information on a computer system. The data manager controls an access list, which contains the identifiers of the users, where the data manager may provide writing access of the user's authorized access. The data manager application is invoked when user desires to access to files (Col 3, lines 15-34; Col 4, lines 49-55).

22. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Desai and Kramer because both teachings deal with providing clients selective access to information stored on a computer network. Furthermore, the teachings of Kramer for a user to provide an identifier and to modify the authorized user's access conditions would improve the teachings of Desai by allowing clients to modify user information as needed, and Kramer's teachings would increase the security of Desai's teachings by preventing unauthorized users to different forms of access.

23. Claims 15-19, 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Orita, US Patent #5,163,147 in view of Desai.

24. As per claim 15, Orita teaches substantially the invention as claimed including a method for selectively allowing access to files over a computer network. Orita's teachings comprise of:

operatively receiving at the host computer a request from the client to access information in the data store (Col 3, lines 10-13, 56-61. Host computer receives a request from the client to access specified files.);

determining an intended use by the client of the information in the data store (Col 4, lines 16-18, 60-63. Client provides data indicating the access type, where access type can be deleted, modifying, writing, and reading.);

determining an allowed level of access permitted by the user (Col 4, lines 34-36, 52-67. Host computer determines the authority level and the access type of user based on the access protection information.);

comparing the determined intended use with the determined allowed level of access (Col 4, lines 34-36, 52-67. Host computer determines the authority level and the access type of user based on the access protection information.), and

completing the request from the client to access information in the data store when the determined intended use by said client of the certain information is within the determined allowed level of access permitted by the user (Col 4, lines 15-19, 52-55. Client requests access to certain files. Col 4, lines 64-68. Request is completed if the type of access is allowed.).

25. Orita teaches of receiving requests to access certain information. However Orita does not teach of receiving at a web-services provider a request from a client, wherein the request is to access information that is specifically certain user-specific information.

26. Desai teaches of providing user-specific information to a client, where the user selectively grants access to the user's user-specific information to one or more clients on an

element-by-element basis. The elements comprise of telephone number, street address, and credit cad number (Col 9, lines 10-18). The user's user-specific information is stored on an information exchange server, accessible through the Internet (Col 8, lines 27-41).

27. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Orita and Desai because both teachings deal with providing selectively allowing access to certain information stored on a database to one of more clients. Furthermore, the teachings of Desai for the information to be user-specific; allowing access to certain information; and storing user-specific information on a web server would improve the teachings of Orita by allowing the user's profile information to be easily accessible to a plurality of clients using the Internet and allowing various types of information to be stored on the data base. The teachings of Desai to provide access to certain user-specific information would allow the user maintain privacy of its information.

28. As per claim 16, Orita teaches the method of claim 15 wherein determining the intended use by the client of the certain user-specific information in the data store comprises: determining a type of information within the certain user-specific information in the data store that is being requested by the client; and determining a form of access to the certain user-specific information in the data store that is being requested by the client (Col 3, lines 56-69; Col 4, lines 16-19. Client request information by specifying a file name and indicates type of access.).

29. As per claim 17, Orita teaches the method of claim 16 wherein comparing the determined intended use with the determined allowed level of access comprises: determining if the user permits access to the type of information within the certain user-specific information in the data store that is being requested by the client; and determining if the user permits the form

of access to the certain user-specific information in the data store that is being requested by the client (Col 3, line2 – Col 4, lines 8; Col 4, lines 55-64. Host computer determines if the client is permitted access to the type of information being requested and determines if the form of access is permitted.).

30. As per claim 18, Orita teaches the method of claim 17 further comprising: creating an access filter, said access filter defining an extent to which the user permits access to the type of information within the certain user-specific information in the data store and an extent to which the user permits the form of access to the certain user-specific information in the data store (Col 3, lines 33-52. Host computer creates an authority level, indicating an extent to which the host computer permits access to the type of information and, an authority level-altering data.); and

wherein completing the request from the client to access the certain user-specific information in the data store when the determined intended use is within the determined allowed level of access further comprises (Col 3, line 1- Col 4, lines 8. The allowed level of access is determined by comparing the authority level needed and the requesting authority level.):

applying the access filter to the user-specific information in the data store to create a filtered information set; and permitting the client to access filtered information set (Col 3, lines 41-52. Files having a certain level are permitted access.).

31. As per claim 19, Orita teaches the method of claim 15 further comprising denying the client access to the requested certain user-specific information in the data store if the determined intended use is outside the allowed level of access (Col 3, line 1–Col 4, line 3; Col 4, lines 52-64. Client is denied if the authority level is outside the allowed level of access.).

32. As per claim 21, Orita teaches one or more computer-readable media having computer-executable instructions for performing the method recited in claim 15 (Col 2, lines 58-60. Host computer performs the necessary process for the invention.).

33. Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Orita and Desai, in view of Kramer.

34. As per claim 20, Orita does not teach the method of claim 15 further comprising invoking a consent engine if the determined intended use is outside the allowed level of access, said consent engine informing the user of the client's request to access the certain user-specific information in the data store and inviting the user to permit or deny the client's request to access the certain user-specific information in the data store.

35. Kramer teaches of protecting data in a computer system, where a data manager can update the access control list to add or remove clients and to permit or deny the client's type of access (Col 4, lines 1-5, 52-55).

36. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Orita, Desai, and Kramer because all three teachings are similar in that they deal with providing selective access to information. Orita teaches of providing access based on an access protection information, where a client is granted access if the client meets the parameters of an access list. Thus, it would be desirable for Orita's invention to also update the access list to allow read or write conditions because Kramer's teachings would improve the system of Orita and Desai by providing greater administrative control to the user by determining who can and cannot access information.

37. Claims 1-3, 7, 8, 10, 14, 29, 30, 35-36, 39, and 44-46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Orita in view of Desai and Bradee et al, US Publication #2002/0095571 (Bradee hereinafter).

38. As per claims 1, 29, 38, 44, 45, and 46, Orita teaches substantially the invention as claimed including a method and a system for selectively allowing access to files over a computer network. Orita's teachings comprise of:

host computer maintaining a data store of information (Col 2, line 66 – Col 3, line 9. Host computer stores files.), said host computer maintaining an access control list identifying when the host computer grants a form of access to a client wherein the form of access granted to the client is limited to certain information (Col 4, lines 52-55. Host computer determines whether access to the file request is permitted.);

obtaining an access request message from the client and directed to the software service requesting user-specific information, said request message including an access request parameter indicating the client's requested form of access to the certain information in the data store (Col 4, lines 16-18, 23-24. Client sends request to access information e.g. specified files, indicating the type of access.);

comparing the access request parameter to an access control list associated with the software service, said access control list identifying whether the user has granted the form of access requested by the client (Col 4, lines 34-36, 52-55, 60-64. Determines if the client has permission based on access protection level.);

permitting the client to have access to the requested certain information in the data store if the user has granted the form of access requested by the client (Col 4, lines 66-67. Client is permitted access if the type of access is granted.); and

invoking an access control engine if the user has not previously granted the form of access requested by the client, said access control engine (Col 4, line 65-Col 5, line 1. Host computer determines if client is provided the form of access by either allowing or denying access.):

determining an intended use by the client of the requested certain information in the data store (Col 4, lines 16-18, 60-62. Client indicates type of access such as read or write.);

comparing the determined intended use by the client of the certain information with a default access control instruction (Col 4, line 65-Col 5, line 1. Determines if client is provided the form of access by either allowing or denying access based on access protection information.);

transmitting a fault response to the client if the default access control instruction does not permit the determined intended use (Col 4, line 68- Col 5, line 1. Access is denied.).

39. Orita teaches of a host computer maintaining a data store of information. However, Orita does not teach of providing a user access to a service provided by a web-services provider, the web-services provider maintaining a data store of user-specific information associated with the user in connection with service, the web-services provider maintaining an access control list identifying when the user grants a form of access to a client wherein the form of access granted to the client is limited to certain user-specific information.

40. Desai teaches of selectively granting access to information, wherein a user has access to a service provided by a web-services provider (Col 8, lines 29-41), a information exchange system maintaining a data store of user-specific information (Col 8, lines 56-62), and the information exchange system selectively granting a form of access to one or more third parties

wherein the access is limited by element-by-element basis, e.g. telephone number, street address, credit number, and business contact (Col 9, lines 10-18).

41. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Orita and Desai because both teachings deal with providing selective access to information stored on a database. Furthermore, the teachings of Desai to perform the above steps in paragraph 40 would improve the teachings of Orita by allowing the information to be easily accessible to a plurality of clients using the Internet and allowing various types of information to be stored on the data base. The teachings of Desai to provide access to certain user-specific information would allow the user maintain privacy of its information.

42. Orita also does not teach of dynamically updating the access control list to permit the client to have access to the requested user-specific information in the data store if the default access control instruction permits the determined intended use allowed by the user.

43. Bradee teaches of dynamically updating an access control list to permit the client to have access to information on a web server if the instructions permit the client for viewing of the information (Page 8, Paragraph 62).

44. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Orita, Desai, and Bradee because all three teachings are similar in that they deal with providing selective access to information. Furthermore, the teachings of Bradee to dynamically update the user access list would improve the system of Orita and Desai by allowing clients to access information that wasn't previously accessible when the clients did not meet predefined parameters.

45. As per claim 2, Orita teaches the method of claim wherein comparing the determined intended use by the client with the default access control instruction further comprises comparing the client's requested form of access to the default access control instruction to determine if the default access control instruction permits the requested form of access (Col 4, lines 52-67. Determines access by comparing the intended use by the client and the access conditions to which the client is allowed.).

46. As per claim 3, Orita teaches the method of claim 1 wherein the client's requested form of access to the user-specific information in the data store identifies a desired subject matter to be accessed and a method of accessing the desired subject matter and wherein comparing the determined intended use by the client with the default access control instruction further comprises: determining if the default access control instruction permits the client to access the desired subject matter; and determining if the default access control instruction permits the identified method of accessing the desired subject matter (Col 3, lines 10-13, 40-51; Col 4, lines 16-18, 55-67. Host computer determines if client is allowed access to the file, and determines if the access protection information allows the identified method of accessing the file e.g. deleting, modifying, writing, and reading.).

47. As per claims 7 and 35, Orita teaches the invention further comprising authenticating a digital identity of the user and denying access to the requested user-specific information in the data store if the digital identity of the user is not authenticated (Col 3, lines 10-14, 56-59. User provides ID information and password. Access is denied if the identity of the user is not authenticated.).

48. As per claims 8 and 36, Orita teaches the invention, wherein determining the intended use by the client of the requested user-specific information further comprises obtaining a copy of an intentions document associated with the client, said intentions document including a field being indicative of the intended use by the client of the requested user-specific information (Col 4, lines 16-18, 57-68. Client sends data indicating access type to the host computer. With the information host computer can determine if access is allowed.).

49. As per claim 10, Orita teaches the method of claim 1 wherein permitting the client to have access to the requested user-specific information in the data store if the user has granted the form of access request by the client further comprises: permitting the client to read the requested user-specific information in the data store; and permitting the client to write the requested user-specific information in the data store (Col 4, lines 16-18, 60-63. Type of access by the client may be reading and writing the information in the data store.).

50. As per claim 14, Desai teaches one or more computer-readable media having computer-executable instructions for performing the method recited in claim 1 (Col 11, lines 27-46. Information exchange system has software to perform necessary functions.).

51. As per claim 30, Orita does not teach of a system comprising a network communication device having a display interface and a selection menu and wherein the user communicates with the web-services provider via the network communication device.

52. Desai teaches that the network device may be a computer running a web browser application and has a selection menu. The network device is adapted to communicate with the information exchange server (Col 8, lines 14-36; Col 13, lines 53-66).

53. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Orita and Desai because the teachings of Desai to have a display interface and selection menu, on a network device that is connected to the web server would improve the teachings of Orita by allowing the user to select which clients are granted access to user information stored on the web server.

54. As per claim 39, Orita teaches the system of claim 38 wherein the access control interface comprises a service-side fabric associated with the software service provided by the web-services system (Col 4, lines 53-68. Host computer controls access to information stored on database.).

55. Claims 4, 5, 13, 31-34, and 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Orita, Desai, Bradee in view of Kramer.

56. As per claims 4, 5, and 31-34, Orita does not teach the method, wherein the user communicates with the web-services provider via network communication device having a display interface and a selection interface, the method further comprising:

generating an option list having at least one entry therein based on the determined intended use by the client of the requested user-specific information in the data store;

displaying to the user on the display interface of the network communication device an option menu reflecting the generated option list, said option menu prompting the user to accept or reject at least one option using the selection interface of the network communication device;

receiving from the network communication device a selection signal indicative of whether the user accepted or rejected the at least one option; and

creating an access control rule based on the received selection signal, said access control rule defining the extent of access to the requested user-specific information in the data store granted to the client.

creating the access control rule comprises updating the access control list such that the access control reflects whether the user accepted or rejected the at least one option.

57. Kramer teaches of protecting data in a computer system where an access list is created based on intended use by the data manager. The data manager has the option to modify the access list, adding or deleting users, and changing the access permissions for the users. The access list is used to define the extent of access to the requester of the information (Col 3, lines 64-Col 4, lines 1-6, 53-55).

58. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Orita, Desai, Bradee and Kramer because all the teachings are similar in that they deal with providing selective access information. Orita teaches of accessing information based on an access protection information, where a client is allowed access if the client meets the parameters of an access list. Thus, it would be desirable for Orita's teachings to include the method of generating an access list to provide the conditions and having the option of changing the access permission because Kramer's teachings would improve the system of Orita, Desai, and Bradee by providing the user with greater administrative control of clients that can access information.

59. As per claim 13, Orita does not teach the method of claim 1 wherein updating the access control list to permit the client to have access to the requested user-specific information in the data store if the default access control instruction permits the determined intended use further

comprises: updating the access control list to permit the client to read the requested user-specific information in the data store; and updating the access control list to permit the client to write the requested user-specific information in the data store.

60. Kramer teaches wherein the access list is updated to permit the client to read and write the requested data file (Col 4, lines 49-55).

61. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Orita, Desai, Bradee and Kramer because all the teachings are similar in that they deal with providing selective access information. Orita teaches of accessing information based on an access protection information, where a client is allowed access if the client meets the parameters of an access list. Thus, it would be desirable for Orita's teachings to update the access list to change the access permission to allow for reading and writing because Kramer's teachings would improve the system of Orita, Desai, and Bradee by providing the user with greater administrative control of clients that can access information and the type of access that the clients can have.

62. As per claim 37, Orita does not teach the system of claim 36 further comprising: a network communication device having a display interface and a selection menu and wherein the user communicates with the web-services provider via the network communication device; and a consent engine retrieving the client intentions document and generating an option list having at least one entry therein based on the intended use identified in the intentions document, said consent engine displaying on the display interface of the network communication device an option menu reflecting the generated option list, said option menu prompting the user to accept

or reject at least one option displayed on the option menu using the selection interface of the network communication device.

63. Kramer teaches of protecting data in a computer system where an access list is created based on intended use by the data manager. The data manager has the option to modify the access list, adding or deleting users, and changing the access permissions for the users. The access list is used to define the extent of access to the requester of the information (Col 3, lines 64-Col 4, lines 1-6, 53-55).

64. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Orita, Desai, Bradee, and Kramer because all the teachings deal with providing selective access to information. Furthermore, the teachings of Kramer to generating an access list to provide conditions and allowing for the change of access permissions would improve the system of Orita, Desai, and Bradee by providing the user with greater administrative control of its stored profile and allowing the user to determine which clients can access the user's information.

65. Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Orita, Desai, and Bradee in view of Allgeier, US Patent #5,995,972.

66. As per claim 6, Orita does not teach the method of claim 1 further comprising: determining if the client has a local copy of the requested user-specific information in the data store before transmitting the access request message; and retrieving said local copy of the requested user-specific information if the local is available; determining if said local copy of the requested user-specific information is current; and transmitting the access request message only if said local copy of the requested user-specific information is not available and not current.

67. Allgeier teaches wherein a determination is made if a selected data is stored in a first database. If the selected data is available, it is retrieved. The invention checks to see if the selected data in the first database is current. If the selected data is not current or not available, the second database is queried and accessed for the selected data (Col 12, lines 1-10).

68. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Orita, Desai, Bradee, and Allgeier because all the teachings are similar in that they deal with accessing information over a computer network. Furthermore, the teachings of Allgeier to determine if local data is available and to request access to data at secondary location if the data is not available or not current would improve the system of Orita, Desai, and Bradee by allowing information to be retrieved even if it is not located at a first location and providing network efficiency by only transferring information on an needed basis, thus preventing large amounts of data from being transferred on fixed bases.

69. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Orita, Desai, and Bradee in view of Robertson.

70. As per claim 9, Orita and Desai teach of determining a client has an access right to the requested user-specific information in the data store; and permitting the client to have access to the requested user-specific information if the client has access rights to the requested user-specific information in the data store (Desai. Col 9, lines 10-18). However, Orita and Desai does specifically that the access right is an access subscription right to the requested user-specific information and permitting the client to have access to the requested user-specific information in the data store if the client has access subscription right to the requested user-specific information in the data store.

71. Robertson teaches of managing which clients may have access to user information. The contact manager provides notification of changes to the user's information to the list of clients. The clients are allowed access to the user information (Col 6, lines 48-54; Col 8, lines 17-23, 57-61).

72. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Orita, Desai, Bradee, and Robertson because all the teachings deal with allowing selective access to information over a computer network. Furthermore, the teachings of Robertson to issue a notification to the users in an access list and allowing access to that information would improve the system of Orita, Desai, and Bradee by allowing registered clients to be informed of the user-specific information and allowing the registered clients to access the user's user-specific information.

73. Claims 11 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Orita, Desai, and Bradee, in view of Erickson et al, US Publication #2003/0081791 (Erickson hereinafter).

74. As per claim 11, Orita teaches the method wherein permitting the client to read the requested user-specific information in the data store comprises accessing said requested user-specific information and transmitting a copy of the access requested user-specific information to the client (Col 4, lines 66-68; Col 5, lines 8-12. Client is allowed access to read the requested information on the host computer, where the contents of the information are displayed on screen.). However, Orita does not teach that the information is send in a SOAP message.

75. Erickson teaches of transmitting messages according to the SOAP protocol (Page 2, Paragraph 21).

76. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Orita, Desai, Bradee, and Erickson because the teachings of Erikson to use the SOAP protocol in sending messages would improve the system of Orita, Desai, and Bradee by providing a simplified process of packaging the application data and because of its compatibility, allowing the exchange of data over the Internet.

77. As per claim 12, Orita teaches the method wherein permitting the client to write the requested user-specific information in the data store comprises receiving at the host computer a message from the client identifying the requested user-specific information and writing the identified requested user-specific information in the data store (Col 3, lines 57-60; Col 4, lines 61-68; Col 5, lines 8-13. Client is permitted to write the information in the host computer, where the host computer receives a request for the information and writing the identified information.). However, Orita does not teach of receiving at the web-services provider a SOAP message from the client.

78. Erickson teaches of transmitting messages according to the SOAP protocol (Page 2, Paragraph 21).

79. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Orita, Desai, Bradee, and Erickson because the teachings of Erikson to use the SOAP protocol in sending messages would improve the system of Orita, Desai, and Bradee by providing a simplified process of packaging the application data and because of its compatibility, allowing the exchange of data over the Internet.

80. Claims 42-43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Orita in view of Desai, Bradee and Kramer.

81. As per claim 42, Orita teaches substantially the invention as claimed including a method for selectively allowing access to files over a computer network. Orita's teachings comprise of:

retrieving an intentions document associated with the third party desiring access to the certain information in the data store, said intentions document identifying (Col 3, lines 10-14; Col 3, lines 15-20, 56-61. Clients sends request to access specific files.):

a purpose for which the third party desires access to the certain information in the data store (Col 3, lines 56-65; Col 4, lines 16-19. Client indicates the type of access such as deleting, modifying, write-in, and readout.);

a method by which the third party proposes to access the certain information in the data store (Col 3, lines 56-65; Col 4, lines 16-19. Client indicates the type of access such as deleting, modifying, write-in, and readout.);

an identity of the third party (Col 3, lines 10-13, lines 56-61. User provides ID and password.);

the certain information in the data store to which the third party desires access (Col 3, lines 10-14; Col 3, lines 15-20, 56-61. Clients sends request to access specific files.);

the purpose for which the third party desires access to the certain information in the data store (Col 3, lines 56-65; Col 4, lines 16-19. Client indicates the type of access.);

the method by which the third party proposes to access the certain information in the data store (Col 3, lines 56-65; Col 4, lines 16-19. Client indicates the type of access.);

prompting the user to authorize or deny the third party to access the certain information in the data store (Col 4, lines 51-68. Host computer authorizes or denies the user access to the user information.); and

operatively receiving a selection signal being indicative of whether the user authorized or denied the third party to access the certain information in the data store (Col 4, line 65 - Col 5, line 7. Client is either accepted or denied access to the file.)

82. Orita does not teach that the information is user-specific information.

83. Desai teaches of providing user-specific information to a client, where the user selectively grants access to the user's user-specific information to one or more clients on an element-by-element basis. The elements comprise of telephone number, street address, and credit cad number (Col 9, lines 10-18). The user's user-specific information is stored on an information exchange server, accessible through the Internet (Col 8, lines 27-41).

84. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Orita and Desai because both teachings deal with providing selectively allowing access to certain information stored on a database to one of more clients. Furthermore, the teachings of Desai for the information to be user-specific; allowing access to certain information; and storing user-specific information on a web server would improve the teachings of Orita by allowing the user's profile information to be more accessible to clients. Desai's teachings would also allow for a fast and convenient method for the exchange of information with clients, such as improving methods of transactions.

85. Orita does not teach the value proposition associated with the purpose for which the third party desires access to information that is user-specific information and creating an access

control rule indicative of whether the user authorized the third party to access the user-specific information in the data store.

86. Bradee teaches of selectively allowing access to information stored on a web server where the client pays to view the information. Bradee also teaches of dynamically updating the access list to allow the client access to the stored information (Page 8, Paragraph 0062)

87. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Orita, Desai, and Bradee because all three teachings deal with providing selective access to information over computer network. Furthermore, the teachings of Bradee for the user to offer a value proposition and to dynamically update the user access list would improve the system of Orita and Desai by allowing clients to access certain information on the web server when the client meets conditions set forth by the user.

88. Orita does not teach of displaying the menu entities on the menu on the display interface of the network communication device.

89. Kramer teaches of protecting data in a computer system where the data manager may modify the access list, allowing the data manager to allow or deny access to the information (Col 14, lines 49-55).

90. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Orita, Desai, Bradee, and Kramer because all the teachings are similar in that they all deal with providing selective access to information. Orita teaches of accessing information based on access protection information, where a client is allowed access if the client meets the parameters of an access list. Thus, it would be desirable for the system

of Orita, Desai, and Bradee to have a display menu because Kramer's teachings would allow a method for the user to change the access permission.

91. As per claim 43, Orita teaches the system of claim 42 wherein the access control interface comprises a service-side fabric associated with the software service provided by the web-services system (Col 4, lines 53-68. Host computer controls access to information stored on database.).

Response to Arguments

92. Applicant's arguments filed 7/7/2005 have been fully considered but they are not persuasive. Applicant argued that (1) Desai fails to recognize an "access control rule" which grants selected access to clients/third parties, not according to an element-by-element basis and a person-by-person basis; (2) Orita does not mention of determining an intended client use, comparing the determined intended use by the client with a default access control instruction, and dynamically updating the access control list; (3) Kramer teachings relate to access with respect to an authorized user, not in the context of a client accessing selected information as recited by claim 1; (4) Robertson teaches that access is based on granted permissions, not an access control engine; (5) Applicant requests that the Examiner specify the teachings for combining the Bradee, Alleiger, Robertson, and Erickson references with Orita or Desai; and (6) Examiner's rejection uses impermissible hindsight analysis.

Examiner traverses the arguments:

93. As to point (1), from the Desai reference,

i) Column 9, lines 10-14, "The information exchange system further indicates facilities that allow the registered user to *selectively grant access* to this stored profile data to one or more third parties on an element-by-element basis."

Desai clearly teachings of providing selected access, so an access control rule must be maintained by the information exchange system to allow the selected access to the third parties. Therefore, Desai teaches the limitation of the claims as argued by the Applicant, where the claims generally state of granting selected access. Furthermore, Applicant's arguments that the access is not according to element-by-element basis and person-by-person are not found in the claims. It is noted that the features upon which applicant relies (i.e., Access not according to element-by-element and person-by-person) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

94. As to point (2), from the Orita reference,

ii) Column 4, lines 16-17, "the file password is required for accessing a file since the file contains a password, along with the data indicating the access type."

iii) Column 4, lines 60-65, "The host computer compares the content (deletion, modification, write-in, readout or the like) of the access type which is to be executed by the user program and the password stored in the EP information defining the user program with the contents of access protection information."

As from the above quoted sections ii and iii from the Orita reference, a client provides an access type for accessing files on the host computer, wherein the access type indicates a plurality of types of uses for the file. Orita teaches that the intended use may comprise of "deletion, modification, write-in, readout" of the file. Thus, Orita clearly teaches of an intended use of the access file. Orita also teaches of comparing the intended use with a default access control instruction as the client's access type is compared with the EP information from quoted section iii.

It is noted by the Examiner that determining an intended use of clients and comparing the determined use by the user is well known in the art as Desai teaches that different parties may request access to user-specific information. Business contacts, for performing business with users, are granted access to the user's telephone number, while telemarketers, for telemarketing, are not granted access to the user's information (Col 9, lines 19-31).

Orita does not teach of dynamically updating the access control list, thus the rejection of dynamically updating the access control list was made Orita in view of Bradee. Bradee teaches of:

> vi) Page 8, Column 0062, "In another example of policy-based access control, the security system can evaluate dynamically updated conditions to determine whether a user should permitted access to a resource. For example, a research web site might provide free access to a limited number of pages to all users. Then, upon supplying certain information such as e-mail address, a free user account is generated automatically on the system, and a greater level of access to available research is permitted....

v) Page 8, Column 0062, "The "paid" status of a user's account is dynamically updated in the security system."

Therefore, Bradee teaches of dynamically updating an access list to allow the user to access information on the web site. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

95. As to point (3), Kramer teaches of accessing information that is not specifically user-specific information. However, Desai teaches of clients accessing information that is specifically user-specific information (Refer to above quoted section (i) of Desai). Therefore, claims 25 and 27 were rejected Desai in view of Kramer; claim 20 was rejected Orita and Desai in view of Kramer; claims 4, 5, 13, 31-34, and 37 were rejected Orita, Desai, Bradee in view of Kramer; and claims 42-43 were rejected Orita in view of Desai, Bradee, and Kramer. One cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

96. As to point (4), claim 9 was rejected Orita, Desai, Bradee in view of Robertson, and claim 23 was rejected Desai in view of Robertson. Orita teaches of controlling access to files stored on a host computer (Refer to above quoted section (ii and iii) of Orita). Therefore, an access control engine is present to determine which clients are allowed access to the files. Desai also teaches of controlling access to user-specific information stored on a web server (Refer to above quoted section (i) of Desai). Therefore, an access control engine is also

present to determine which clients are allowed access to the user-specific information. The Robertson reference was used to teach what was not taught in the Orita and Desai references, which was of a subscription status and notifying clients of changes in the user-specific information. One cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

97. As to point, (5) in response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case:

Bradee teachings of providing dynamic update of an access list would provide additional rights to clients, allowing clients access to more information as taught by Bradee (Paragraph 0062).

Allegier teaches that if information is not located at a primary access location, the data is retrieved from a secondary location. Storing data at multiple locations is well known in the art and would be beneficial for a plurality of reasons. The reason would comprise of: providing a backup to the primary server in case the primary server crashes; providing a secondary storage, i.e. a database, where the primary server has limited memory; and allocation of information which would allow for an efficient transfer of data, as taught by Allegier (Col 2, lines 33-42).

Robertson teaches of maintaining a subscription of clients and providing a notification to the clients of updates to a user's information (Col 2, lines 47-52; Col 6, lines 49-55). Desai teaches of storing user-specific information on a web server to allow clients such as business contacts and online vendors to view the user's information. Robertson's teachings would be beneficial because if the user's personal information such as a telephone number or credit number would happen to change, a notification would be send out to the clients of the changes. This would allow an online vendor to charge the new credit card number instead of the old credit card number and would allow business contacts to maintain the correct contact information of the user without having to frequently visit the web server.

Erickson teaches of sending information in the SOAP protocol and the motivation to combine Orita and/or Desai with Erikson may be found in Newton's Telecom Dictionary 19th Edition, 2003. The definition of SOAP in the dictionary states:

> vi) "SOAP simplifies the process of packaging the application data associated with the RPC, and sending it across the Internet. XML tags the content to ensure that both sender and recipient can easily interpret message contents, and SOAP provides specific instructions that allow a network node to remotely invoke application objects and return results... Because SOAP is based on XML, it's compatible with all programming models and allows business to exchange data with each other over the Internet."

98. As to point (6), in response to applicant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge

gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

Conclusion

99. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

100. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

101. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Joshua Joo whose telephone number is 571 272-3966. The examiner can normally be reached on Monday to Friday 7 to 4.

102. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John A. Follansbee can be reached on 571 272-3964. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

103. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

September 14, 2005
JJ

JOHN FOLLANSBEE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100